SysAdmin's Notebook

Supported Compression Formats

Practically everyone who works in a corporate environment will try this trick at least once. Compressing or zipping a file is a common method of circumventing security measures to get past a firewall filter. Maybe you just wanted to see if you could out-smart the firewall, or more likely because you "knew" that your judgment was better than that of the firewall policy in a particular instance.

A common scenario is that a user may wish to run a simple little utility on their desktop that they've used thousands of times on their home computer, but forgot to bring the file to work. Not to worry, it's barely over a hundred Kilobytes and they can probably download it in a matter of minutes. That's when the user gets frustrated, because Network Administrators at work have placed a filter on downloaded material that blocks executable files. So the user rationalizes, *surely they couldn't mean my harmless and very useful app that thousands of other people have downloaded from a website hosting free downloads!* In fact, the website is so accommodating that it gives users the option to download the 750 Kb program in a compressed file format to save valuable bandwidth. Six months later, the legal department is trying to figure out what the company's responsibilities are to customers and shareholders with regard to the data loss of an unknown number of confidential documents due to a rampant Trojan horse attack that breached the company network.

Sometimes, the most important job for IT personnel is to protect people from their own actions. In the scenario above, the decision to filter executable files was made for a good reason. If the filtering can be bypassed simply by selecting a different download option, its effectiveness is somewhat questionable at best. For this reason some firewalls include the capability to uncompress archive files and scan the content in compressed file formats. The ability to scan the content of a compressed file is only one tool in what should be a large and multifaceted toolkit.

Archive and compression file formats

Archive and compression files have been around for decades. There are many types of utilities—free, commercial and shareware—and all with their own specific algorithms. A quick look at Wikipedia shows a large list of formats, including:

- Archiving only formats
- Compression only formats
- Archiving and compression format

This leads to the next logical progression; that choosing one of the formats that the firewall cannot uncompress or un-archive is more likely to get by a firewall's filter policy. Therefore, the more formats your firewall can open the more secure your network is.

Not all Engines are the same

While it may seem a forgone conclusion that every firewall and every AV engine would open every format possible there are differences and limitations. In versions of FortiOS 5.0 and earlier, the two different inspection modes (Proxy-based and Flow-based) use different engines to do the scanning. Because of the way the Flow-based mode works in earlier versions of FortiOS, it opens a more limited number of compression and/or archive formats. Now that both inspection modes use the same improved AV engine in FortiOS 5.2, all of the formats listed below can be opened in both Proxy-based and Flow-based AV modes.

Different products also take different approaches to which formats will be targeted. For instance, some firewalls only check ZIP and GZIP formats. Others may check a few more popular formats, but nowhere near all of the wide variety formats available. In order to check other file formats, they have to proxy the entire file to scan it.

What can a FortiGate do?

The FortiGate AV engine, that looks to filter content on the incoming files, can open the following:

Archive / Compression formats

- ZIP
- ZIPX (BZIP2, INFLATE64, LZMA, LZMA2)
- JAR
- RAR
- 7Z
- BZIP2
- CAB
- TAR
- GZIP
- ARJ
- LZH
- MSC (Microsoft Compress)
- SIS (Symbian Installer Package)
- SISX (Symbian Installer Package for 9.x)
- SWF
- NSIS (Nullsoft Installer Package)
- E32Image (Symbian 9.x, compressed with custom LZW algorithm)
- XZ (starting with AV engine v4.3)
- CPIO (starting with AV engine v4.3)
- AutoIt (starting with AV engine 5.0)
- TNEF (starting with AV engine 5.1)

Self Extracting formats

- SFX ZIP
- SFX RAR
- SFX LZH
- SFX ARJ
- SFX CAB
- SFX 7Z

Static Packers

- UPX
- ASPACK
- PETITE
- FSG

Generic/Custom Packers

The engine supports most custom packers with emulator, including:

- UPACK
- Mew
- PECompact
- ASProtect
- PecBundle
- PEncrypt
- ACProtect

Document formats

Text files are straightforward and easily readable by most editors, but there are some text files that require an editor specifically configured to read these proprietary formats. The following file formats can be read by a FortiGate:

- PDF
- MS OFFICE
- RTF
- WORDML
- MIME

Misc

With anything a diverse as file formats there has to be a miscellaneous section for these that don't really fit in any of the other groupings.

- UNICODE

Levels of compression or archiving

Individuals who attempt to confound the scanning process by compressing a file multiple times will be defeated by the FortiGate's ability to scan through multiple levels of compression. By default, a FortiGate will go through 12 nested levels of compression to find the original file and this setting can be increased to 100 levels.

Before changing the setting to 100, remember that it is unlikely that the file sender will go through the effort to compress a file beyond the default, and the file receiver is even less likely to want to uncompress the file that many times. It takes system resources to go through uncompressing a file, so it might be simpler to drop any files that are nested that many times.